IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

MAGIC LABS, INC., Plaintiff, v. HORKOS, INC. d/b/a PRIVY, Defendant.	Civil Action No. 1:23-cv-00967-RGA **JURY TRIAL DEMANDED**

PLAINTIFF MAGIC LABS, INC.'S ANSWERING BRIEF IN OPPOSITION TO DEFENDANT'S PARTIAL MOTION TO DISMISS PLAINTIFF MAGIC LABS, INC.'S FIRST AMENDED COMPLAINT PURSUANT TO FED. R. CIV. P. 12(B)(6) AND 35 U.S.C. § 101

Dated: February 5, 2024

OF COUNSEL:

Daralyn J. Durie
Ragesh K. Tangri
Timothy C. Saulsbury
Michael Burshteyn
Joyce C. Li
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105
(415) 268-7000

Sara Doudar
MORRISON & FOERSTER LLP
707 Wilshire Blvd., Suite 6000
Los Angeles, CA 90017
(213) 892-5200

MCCARTER & ENGLISH, LLP
Daniel M. Silver (#4758)
Alexandra M. Joyce (#6423)
Renaissance Centre
405 N. King Street, 8th Floor
Wilmington, DE 19801
T: (302) 984-6300
dsilver@mccarter.com
ajoyce@mccarter.com

Attorneys for Plaintiff
Magic Labs, Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. NATURE AND STAGE OF PROCEEDINGS

Privy moves to dismiss Magic's claims asserting the '321 Patent, one of the two asserted patents in this case. Privy argues that the '321 Patent claims ineligible subject matter because it covers the abstract idea of "using software to facilitate set up of third-party storage for digital keys." (D.I. 17 at 1.) Privy oversimplifies the claimed invention. Magic did not simply replace a human intermediary with a software intermediary in an existing system for storing digital keys; it created a new and specific architecture to address particular security vulnerabilities inherent to prior art systems for authentication and key-management in decentralized applications.

II. SUMMARY OF ARGUMENT

Under step one of *Alice*[1], the '321 Patent claims are not directed to an abstract idea. Rather, as shown by the allegations in the First Amended Complaint ("FAC," D.I. 14), they are directed to a solution for a problem that arises in the context of decentralized software applications running across distributed, networked computers: preventing malicious actors from accessing a user's encryption keys, while preserving the user's ability to conveniently access, store, and manage them. Because Privy's arguments ignore those technological benefits and fail to take Magic's well-pled allegations as true, this motion must be denied, and the Court need not proceed to *Alice* step two. Regardless, Privy's motion also fails under step two because the claims contain an inventive concept that renders them patent eligible: they describe a specific implementation of the purported abstract idea that solves a problem unique to computer networks. Privy's contrary argument is premised on multiple factual presumptions that contravene the allegations of the FAC; in short, Privy's step two arguments at best present a factual dispute, which requires denial of its motion.

[1] *Alice Corp. Pty. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014).

III. TECHNICAL BACKGROUND

The '321 Patent provides an "improved system for securing data" in the context of "decentralized applications." '321 Patent (FAC, Ex. A) at 1:41, 1:45–48. Decentralized applications are technologies—such as blockchain—that rely on distributed computing systems not subject to any central authority that controls processes in the system. *See id.* at 1:45–48. A blockchain is a decentralized digital ledger that consist of "blocks" of data in a chain, wherein each block contains the history of data transactions that have occurred as part of the blockchain. (FAC ¶ 8.) Two of the first blockchain applications were cryptocurrencies (such as Bitcoin) and non-fungible tokens ("NFTs"). (*Id.* ¶¶ 9–10.)

Decentralization is the core attribute of blockchains, which secure and authenticate transactions via consensus across independently operated computers (*id.* ¶ 8), in contrast to traditional systems that rely on one trusted central authority (such as a bank or mint) (*id.* ¶ 28). If one computer is compromised, the others can reference the entire blockchain to protect against fraudulent or malicious changes. (*Id.*) Each user controls their blockchain-based digital assets with a private encryption key, which is used to sign transactions and prove ownership. (*Id.* ¶ 22.) The private key itself is essentially the digital asset: whoever controls the private key controls the asset. (*Id.* ¶ 23.) Key security is thus paramount; as the '321 Patent notes, "it can be very difficult, often impossible, to recover from loss or theft of a private key." '321 Patent at 3:38–40.

These general principles were set forth in the Bitcoin white paper published in 2008. (FAC ¶ 21.) The white paper did not, however, provide a solution for managing private keys, which is necessary to perform blockchain-based transactions. (*Id.* ¶ 24.) At the time of Magic's invention, users' existing options each had serious drawbacks. (*Id.* ¶¶ 25–30.) Most notably, all the options involved a direct link between the process that generates the key and the application

that is using the key, which exposed the key to malicious actors who could, for example, access the key by hacking the user's device or a centralized server. (*Id.* ¶ 30.) The '321 Patent addresses these vulnerabilities in the prior art by providing "an improved system for securing data" in the context of decentralized applications such as blockchains. '321 Patent at 1:45–55. Specifically, the '321 Patent provides a system for authenticating a user to securely access the user's keys wherein the authentication system is "non-custodial"—meaning it does not ever have custody of the user's keys. *See id.* The authentication system provides additional protection against attacks on the user's device—which otherwise might be directly linked to the third-party system storing the user's keys. At the same time, the authentication system is not itself a "centralized computing system" that is vulnerable to attack. *Id.*

IV. LEGAL STANDARD

The Supreme Court has set forth a two-step framework for determining patent eligibility under 35 U.S.C. § 101. *Alice Corp.*, 573 U.S. at 217–18. First, the court must determine whether the claims at issue are directed to a patent-eligible concept, such as an abstract idea. *Id.* Second, if the claims are directed to an abstract idea, the court must determine whether the claims contain an "inventive concept—i.e., an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself." *Id.* (cleaned up). Patent eligibility can only be determined on a motion to dismiss "when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law." *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018). Plausible factual allegations preclude dismissal where "nothing on the record refutes those allegations as a matter of law or justifies dismissal under Rule 12(b)(6)." *Id.* (cleaned up). Plausible factual allegations in the complaint may also create a dispute of fact as to whether an inventive concept exists under *Alice* step two. *IPA Techs., Inc. v.*

Amazon.com, Inc., 352 F. Supp. 3d 335, 343 (D. Del. 2019).

V. ARGUMENT

A. *Alice* Step One: The Claims Are Directed to Improved Security for Encryption Keys in Decentralized Applications

Privy argues that the '321 Patent claims are directed to the abstract idea of "using a software program to facilitate setting up a third-party key storage." (D.I. 17 at 6, 19–20.) Privy oversimplifies the claimed system to characterize it as abstract and misses the core benefit of the claimed invention over the prior art. *See IOENGINE, LLC v. PayPal Holdings, Inc.*, 607 F. Supp. 3d 464, 485 (D. Del. 2022) (characterization of claims as directed to "the abstract idea of transmitting messages through an intermediary" "summariz[ed] the claimed subject matter at too high a level of abstraction to fairly represent what the claims actually recite."). The '321 Patent's claimed invention did not simply introduce a software intermediary to an existing key storage system, but fundamentally changed the architecture of the existing systems. As detailed below, the claimed invention is directed to a solution for a problem that arises in the context of decentralized applications running across distributed, networked computers: preventing malicious actors from accessing a user's encryption keys, while preserving the user's ability to conveniently store and access them. That the claimed invention ***thereby*** improved user experience does not negate this technical advance (contrary to Privy's repeated suggestion otherwise, *e.g.*, D.I. 17 at 3, 11, 13, 18).

1. The Claims Solve a Problem Specific to Computer Networks

Prior to Magic's invention, there were four options for managing encryption keys: (1) using a standalone, physical computing device known as a hardware security module ("HSM"); (2) using a third-party HSM (via a third-party key storage system); (3) using a third-party server; and (4) using a browser extension or mobile application. (FAC ¶ 25.) Privy

only addresses the second option, arguing that Magic's advance is simply having a software service provider facilitate the setup of key storage via an access token—and thus the invention is directed at the "*idea* of facilitating the set up of third-party key storage." (D.I. 17 at 7.)

As a threshold matter, Privy's focus on the prior art third-party HSM system is misplaced because that was not a genuine solution for the types of users who benefit from the technological solution supplied by Magic's invention. In that prior art system, the user interacts directly with the third-party key storage provider, meaning the user bears the burden and expense of building the infrastructure necessary to securely access the third-party key storage system—something few users would be willing to take on. (FAC ¶ 27.) The overwhelming majority of relevant users instead would have used the conventional third-party server option, which was a direct-to-consumer service that managed key generation and storage for the user. (*Id.* ¶ 28.) This conventional system suffered from serious security risks, however, due to its centralized nature: the user's keys could be accessed on the third-party server using the user's password credentials. (*See id.*) Even if the credentials were encrypted, a malicious actor could infiltrate the server, download the encrypted credentials, crack the encryption offline at their leisure, and then use the credentials to access the user's keys at the server. (*See id.*) The claimed invention recites a technological solution to this problem by providing a new system architecture in which: (1) the encryption key is generated at the client device ("generating a key by the client"); (2) the encryption process is performed on a third-party computer system rather than on the authentication system where the keys could be compromised and downloaded ("sending over the network from the client to the third party key storage system . . . one or more messages that include the access token, the key, and a request to encrypt the key"); and (3) the authentication system is bypassed in that encryption process ("bypassing the authentication system").

Regardless, even under Privy's contrived framework that focuses on the prior art third-party HSM system, Privy's arguments fail because they do not account for the critical distinctions between that system and '321 Patent's claimed invention set forth in the FAC. As noted above, in the prior art system, the user interacts directly with a third-party key storage provider (without a separate authentication system). (*Id.* ¶ 27.) The prior art system is thus vulnerable to cyberattacks because there exists a direct link between the user's device and the key storage system. (*Id.* ¶ 30.) This direct link allows a malicious actor to access the user's keys by, for example, taking over the user's device to request the keys from the key storage system. (*See id.*)

Magic's claimed invention reduced the security risks posed by both the third-party server and third-party HSM systems in the prior art by introducing a ***non-custodial*** authentication system. (*See id.* ¶¶ 30–39.) Specifically, representative claim 11 states:[2]

> 11. A non-transitory computer readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method to ***setup a wallet for a decentralized application by performing a non-custodial authentication method for a client***, the method comprising:
>
> sending, over a network by ***the client to an authentication system, a sign-up request*** for a user account associated with the decentralized application;
>
> receiving over the network ***at the client from the authentication system, an access token*** that corresponds to the sign-up request, ***for use at a third party key storage system***;
>
> generating a key by the client; and
>
> sending over the network from ***the client to the third party key storage system and bypassing the authentication system***, one or more messages that include ***the access token, the key, and a request to encrypt the key***.

It is clear from the preamble that claim 11 addresses a problem that is specific to computer

[2] The parties agree that claim 11 is representative for the purposes of assessing patentability under § 101. (D.I. 17 at 4 n.3.)

networks: the preamble expressly states that the processor performs "a method to setup a wallet for a ***decentralized application***." The specification explains that a decentralized application is a "decentralized computer application[] that execute[s] on a distributed computing system." '321 Patent at Abstract, 1:45–48, 2:59–62. In other words, the claimed invention provides a system for setting up a wallet specifically in the context of a computer application executed on a particular type of computer network—a decentralized distributed computing system. The body of claim 11 then specifies how that system is structured to accomplish that purpose. *See 01 Communique Lab'y, Inc. v. Citrix Sys., Inc.*, 151 F. Supp. 3d 778, 795 (N.D. Ohio 2015) (claim not directed to an abstract idea where "[t]he preamble describes the use and purpose of the claimed computer product" and the body of the claim "specifies how the claimed computer program product accomplishes the solution of the [patented invention]").

The system of claim 11 is further illustrated in Figure 2A of the '321 Patent:

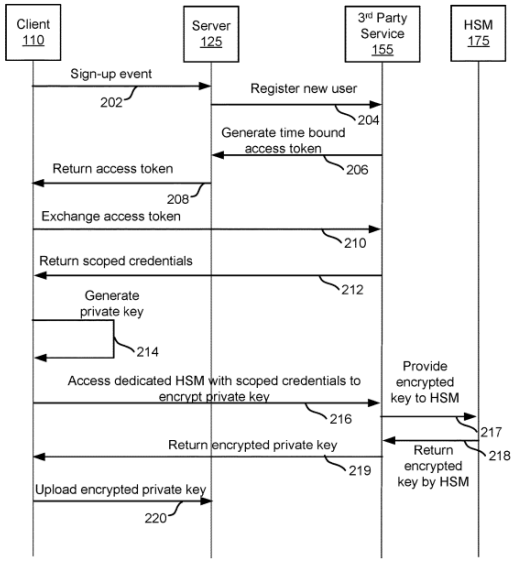


FIGURE 2A

As shown in Figure 2A, instead of having a direct connection between the client device and the third-party key storage system, the client device must first request and receive from an

authentication system (server 125) an "access token…for use at [the] third party key storage system" (third-party service 155). '321 Patent, claim 11; *id.*, Fig. 2A (steps 202, 204, 206, and 208). The client device then generates the user's key (Fig. 2A, step 214), and sends the access token along with the key and a request to encrypt the key to the key storage system, "bypassing the authentication system" (Fig. 2A, steps 210 and 216). '321 Patent, claim 11. The claimed invention thus creates an additional layer of protection for the user's keys that did not exist in the prior art third-party key storage system: because there is no longer a direct link between the user and key storage system, instead of simply taking over the user's device, a malicious actor would now need to infiltrate both the client device and authentication system in order to obtain an access token to request the user's keys from the key storage system.

The use of an authentication system alone, however, would not have addressed the security vulnerabilities in the prior art: an authentication system with access to a user's keys is a version of the third-party server system in the prior art, which carried substantial security vulnerabilities due to its reliance a centralized server. (*Id.* ¶¶ 28, 30.) The '321 Patent addressed that problem by requiring a "non-custodial" authentication system, which never has access to the user's keys. '321 Patent, claim 11 ("a method to setup a wallet for a decentralized application by performing a ***non-custodial authentication*** method for a client"). The authentication system never receives the key from the user because the key is generated at the client device and then sent to the key storage system, "bypassing the authentication system." *Id.* And the authentication system cannot request the key from the key storage system on its own because the key storage system requires an "access token that corresponds to the sign-up request" by the user. *Id.* As the '321 Patent specification explains, the access token allows the client device to "directly communicate" with the key storage system (third-party service 155); the authentication

system (server 125) is "bypassed" in the client device's communications with the key storage system and "cannot forge or intercept" the credentials the key storage system provides the client device to access the user's keys. '321 Patent at 4:46–66. As a result, unlike in the conventional third-party server system, a malicious actor cannot access the user's keys by infiltrating the authentication system alone, but would need to infiltrate both the authentication system and client device to request the keys from the third-party key storage system.

The '321 Patent claims are thus not directed to the abstract idea of "using a software program to facilitate setting up a third-party key storage," as Privy contends (D.I. 17 at 6), but are directed to a solution for a problem that arises in the context of decentralized applications running across distributed, networked computers, analogous to the claims the Federal Circuit upheld in *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245 (Fed. Cir. 2014) and *SRI International, Inc. v. Cisco Systems, Inc.*, 930 F.3d 1295 (Fed. Cir. 2019).

In *DDR Holdings*, the court addressed a patent claim that recited a system wherein "upon the click of an advertisement for a third-party product displayed on a host's website, the visitor is no longer transported to the third-party's website," but instead is sent to a "hybrid web page that combines visual 'look and feel' elements from the host website and product information from the third-party merchant's website." *Id.* at 1257–58. The court held that the claimed system was not directed to the abstract concept of a "store within a store"—wherein the real-world analog was a third-party kiosk in a warehouse store—because the problem solved by the claimed system was specific to the context of computer networks. Engaging with a third-party kiosk in a warehouse store does not instantly transport the visitor to a new venue associated with the third party where the visitor can make a purchase "without any indication that they were previously browsing the aisles of the warehouse store, and without any need to 'return' to the aisles of the store after

completing the purchase." *Id.* at 1258. The solution offered by the claimed system—means to "retain[] control over the attention of the customer in the context of the Internet"—was thus "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *Id.* at 1257–58.

The same reasoning applies to the '321 Patent claims: the solution offered by the claimed invention is necessarily rooted in computer technology because it addresses a problem (vulnerability to cyberattacks) specific to the context of computer networks (management of encryption keys for a "decentralized application"—a computer application executing on a decentralized distributed computing system). That problem does not exist in the "brick and mortar" context because there is no real-world analog to a decentralized distributed computing system—and thus no need for consumers to securely generate, store, and access encryption keys to perform transactions in such a system. The security challenges solved by the claimed invention are unique to the realm of computer networks.

SRI International addressed a claim that recited a method for monitoring a computer network for suspicious activity. *SRI Int'l, Inc. v. Cisco Sys., Inc.*, 930 F.3d 1295, 1301 (Fed. Cir. 2019). Cisco argued that SRI's claims were directed to the abstract idea of "analyzing data from multiple sources to detect suspicious activity." *Id.* at 1303. The Federal Circuit disagreed, finding instead that "[t]he claims are directed to using a specific technique—using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors—to solve a technological problem arising in computer networks: identifying hackers or potential intruders into the network." *Id.* The '321 Patent claims are similarly directed to using a specific technique—use of a "non-custodial" authentication system to provide access tokens necessary to request the user's keys from a third-party key storage system, wherein

the authentication system does not itself have access to the user's keys—to solve a technological problem arising in computer networks—preventing malicious actors from accessing encryption keys.

Numerous cases in this District (and others) have upheld similar claims for the same reasons. *See, e.g.*, *PalTalk Holdings, Inc. v. Riot Games, Inc.*, No. CV 16-1240-SLR, 2017 WL 2106124, at *5 (D. Del. May 15, 2017) (solved a problem "unique to the world of interactive software applications shared over a computer network"); *KOM Software Inc. v. NetApp, Inc.*, No. CV 18-160-WCB, 2023 WL 6460025, at *7–8 (D. Del. Oct. 4, 2023) (solved a computer network problem of "eliminating errors that may occur when attempting to access a storage medium"); *Droplets, Inc. v. Yahoo! Inc.*, No. 12-CV-03733-JST, 2022 WL 20016849, at *3 (N.D. Cal. Aug. 25, 2022) (solved a computer network problem of retaining information entered into a website that would be lost after the user left the site); *DataTern, Inc. v. Microstrategy, Inc.*, No. CV 11-11970-FDS, 2015 WL 5190715, at *8–9 (D. Mass. Sept. 4, 2015) (solution for "mapping between an object-oriented program and a relational database" was computer-specific because such programs and databases are used primarily, if not exclusively, on computers); *01 Communique*, 151 F. Supp. 3d at 795 ("a specific solution to remote access problems" was rooted in computer technology); *Comcast Cable Commc'ns, LLC v. Sprint Commc'ns Co., LP*, 203 F. Supp. 3d 499, 527 (E.D. Pa. 2016) (solved a "technological problem unique to a particular cellular network implementation"); *Rich Media Club LLC v. Duration Media LLC*, No. CV-22-02086-PHX-JJT, 2023 WL 4489270, at *6–7 (D. Ariz. July 12, 2023) (claims directed to a technological solution because "[t]here is no direct pre-computer analog" to the problem solved).

2. Privy's Arguments Raise a Factual Dispute and Cannot Support Dismissal

The allegations in the FAC—which must be accepted as true for purposes of deciding this

motion—describe the problems that existed in the prior art systems and technological benefits of the claimed system. (*See* FAC ¶¶ 25–39.) As detailed above, those allegations demonstrate that the '321 Patent claims are directed to a technological solution for a problem that arises in the context of decentralized applications running across distributed, networked computers. Privy's arguments to the contrary are premised on the assumption that these allegations instead demonstrate that the claims are directed to an abstract idea. In other words, Privy raises a factual dispute over what existed in the prior art and how the '321 Patent claims improved upon that prior art, which cannot be resolved on this motion. Privy's arguments should thus be rejected. *See Aatrix*, 882 F.3d at 1125 (a Rule 12(b)(6) motion should be denied in view of factual allegations that, taken as true, prevent resolving patent eligibility as a matter of law).

In particular, Privy makes three distinct arguments. First, Privy relies on *Alice* and *LendingTree, LLC v. Zillow, Inc.*, 656 F. App'x 991 (Fed. Cir. 2016) to argue that the '321 Patent claims are directed to the abstract idea of software facilitation of a known process: "connect[ing] the client with a third-party storage provider…and direct[ing] the client to carry out the long-prevalent concept of setting up third-party key storage." (D.I. 17 at 7–9, 11, 14). Not so. The allegations in the FAC show that the claims do not simply use software to implement an existing third-party key storage system but address a particular security vulnerability in the prior art systems by requiring the use of a non-custodial authentication system. Thus, unlike the claims in *Alice* and *Lending Tree*, Magic's claimed invention does not merely substitute software for a human in a known process: Magic fundamentally changed the architecture of the existing processes, which were necessarily rooted in the context of computer networks (decentralized applications executed on distributed computing systems), by specifying the particular interactions between a user's device, an authentication system, and a third-party

key storage system, such that the authentication system provides access tokens to the user for the user to access their keys at a third-party key storage system without also having access to the user's keys, to improve the security of the overall computer network. *Cf. Alice*, 573 U.S. at 219–220 (claims directed to "the use of a third party to mitigate settlement risk" wherein software plays the role of the third party); *LendingTree*, 656 F. App'x at 996 (claims directed to the abstract idea of "coordinating loans" using a "computer program on a loan-processing computer" in place of a human broker).[3]

Second, Privy relies on *Electric Power, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) and its progeny to argue that the '321 Patent claims are directed to the abstract concept of "generic data transmission and manipulation." (D.I. 17 at 9–10.) Specifically, Privy asserts that the claims just recite "information transmission between a client (*e.g.*, an end user's computer) and an authentication system" and "generating credentials and sending them (along with the access token) to a trusted third party for storage." (D.I. 17 at 9–10.) This is another example of Privy's (improper) oversimplification of the claimed system, contrary to the allegations in the FAC. In *Electric Power*, the claimed invention's purported advance over the prior art was "a process of gathering and analyzing information of a specified content, then displaying the results" itself, "not any particular assertedly inventive technology for ***performing*** those functions." *Id.* at 1354 (emphasis added). In contrast, the '321 Patent claims are not about mere data transmission and manipulation; they are about a set of computer systems with specific interactions (client, non-custodial authentication system, and third-party key storage system),

[3] Privy also cites *BroadSoft, Inc. v. CallWave Commc'ns, LLC*, 282 F. Supp. 3d 771 (D. Del. 2017), *GoDaddy.com LLC v. RPost Commc'ns Ltd.*, No. CV-14-00126-PHX-LAT, 2016 WL 3165536 (D. Ariz. June 7, 2016), and *Card Verification Solutions, LLC v. Citigroup Inc.*, No. 13-C-6339, 2014 WL 4922524 (N.D. Ill. Sept. 29, 2014) for the same proposition as *Alice* and *LendingTree*. (D.I. 17 at 8 & n.4). Privy's reliance on those cases fails for the same reasons.

wherein the nature of those interactions yields concrete improvements to the security of the computer network. *See TakaDu Ltd. v. Innovyze, Inc.*, No. CV 21-291-RGA, 2022 WL 684409, at *5 (D. Del. Mar. 8, 2022) (distinguishing the challenged claims from those in *Electric Power* that "merely instruct the user to analyze the data"). Regardless, that a claim involves gathering and analyzing data does not, by itself, mean that the claim is directed to an abstract idea. *See id.*

Finally, Privy argues that the '321 Patent claims cannot be directed to an improvement in computer technology because they fail to explain how any technological improvement is achieved. (D.I 17 at 11–14.) Privy asserts that the use of a "non-custodial intermediary" is not an improvement to computer functionality because "having a user generate keys locally and then store then with a third-party key storage system was well known prior to the '321 patent" and thus "it was known in the prior art for authentication systems not to have access to the user's keys." (*Id.* at 13–14.) But, contrary to Privy's assertions, the FAC makes clear that the prior art third-party key storage system did not involve any authentication system separate from the user: the user interacted directly with the key storage provider. (FAC ¶ 27.) Although it is true that this means no authentication system had access to the user's keys, it also made the user's device vulnerable to attack because it had a direct link to the third-party key storage provider. The '321 Patent claims provide a technological improvement by addressing that security concern, without creating new vulnerabilities through the authentication system, and expressly recite how to implement that improvement—by using a "non-custodial" authentication system to provide access tokens necessary to request the user's keys from a third-party key storage system, wherein the authentication system does not itself have access to the user's keys. The '321 Patent claims are thus distinguishable from those in Privy's authorities, which fail to recite any technological improvement, let alone explain how it is implemented. *Cf. Apple, Inc. v. Ameranth, Inc.*, 842

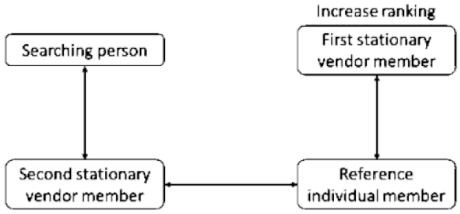
F.3d 1229, 1244 (Fed. Cir. 2016) (claims "cover the process of a restaurant server taking an order from a customer and keeping track of what customer placed that order, when done using a computer"); *In re TLI Commc'ns LLC Pat. Litig.*, 823 F.3d 607, 612 (Fed. Cir. 2016) (claims "directed to the use of conventional or generic technology in a nascent but well-known environment, without any claim that the invention reflects an inventive solution to any problem presented by combining the two"); *Universal Secure Registry LLC v. Apple Inc.*, 10 F.4th 1342, 1349 (Fed. Cir. 2021) (claims "do not purport to improve any underlying technology"); *Prism Techs. LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014, 1017 (Fed. Cir. 2017) (claims do not "cover a concrete, specific solution to a real-world problem"); *Free Stream Media Corp. v. Alphonso Inc.*, 996 F.3d 1355, 1365 (Fed. Cir. 2021) ("the alleged technological improvement does nothing more than implement a computer to achieve the abstract idea of providing targeted advertising to the mobile device user"); *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 774–75 (Fed. Cir. 2019) ("claims do nothing to improve how charging stations function; instead, the claims merely add generic networking capabilities to those charging stations and say 'apply it'"); *Rady v. Bos. Consulting Grp., LLC*, No. 1:20-CV-02285 (ALC), 2022 WL 976877, at *3 (S.D.N.Y. Mar. 31, 2022) (claims merely recite the use of blockchain for gemstone data without describing "how the patent improves blockchains").

B. *Alice* Step Two: The Claims Contain an Inventive Concept that Renders Them Patent Eligible

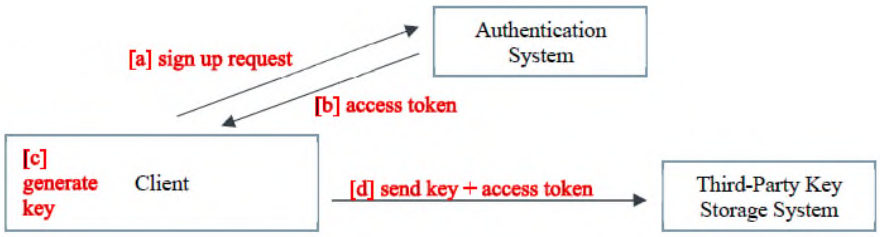
Because the claims are not directed to an abstract idea, the claims pass muster under *Alice* step one—and Privy's motion should be denied on that basis alone. As demonstrated below, Privy's motion should also be denied for the independent reason that the claims contain an inventive concept that renders them patent eligible under *Alice* step two.

Weisner v. Google LLC, 51 F.4th 1073 (2022) is instructive. In that case, the Federal

Circuit found the claims at issue directed to the abstract idea of "creating and using travel histories to improve computerized search results." *Id.* at 1084. But the Federal Circuit reversed the district court's dismissal on the pleadings under *Alice* step two, finding the claims "recite a specific implementation of the abstract idea that purports to solve a problem unique to the Internet." *Id.* at 1085. In particular, the claims describe the use of a "'physical location relationship' with a third-party 'reference individual' to increase the priority of search results." *Id.* at 1086. The court concluded that this "is more than just the concept of improving a web search using location history—it is a specific implementation of that concept." In support, the court noted that even "Google recognizes the specificity of this process with the following diagram from its appeal brief 'illustrat[ing] the relationships.'" *Id.*



The same analysis applies to the '321 Patent claims. Even assuming *arguendo* that the claims are directed to the abstract idea of "using a software program to facilitate setting up a third-party key storage" (D.I. 17 at 6), they describe a specific implementation of that abstract idea that solves a problem unique to computer networks: the use of an authentication system to provide access tokens necessary to request the user's keys from a third-party key storage system, wherein the authentication system does not itself have access to the user's keys—in order to address security vulnerabilities in the prior art. And, similar to Google in *Weisner*, Privy recognizes the specificity of this system with its diagram from its opening brief (D.I. 17 at 4):



Privy argues that the individual components of the '321 Patent claims are conventional and thus cannot provide an inventive concept under *Alice* step two. (D.I. 17 at 14–17.) But *Alice* makes clear that the inventive concept may be supplied by the elements of a claim either individually or "as an ordered combination." *Alice*, 573 U.S. at 217. Indeed, Privy concedes (as it must) that "an inventive concept can be found in the non-conventional and non-generic arrangement of known, conventional pieces" (D.I. 17 at 17). *BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1350 (Fed. Cir. 2016). Privy contends, however, that the '321 Patent claims lack an inventive concept because their "supposedly inventive architecture is nothing but the abstract idea itself—having a software intermediary facilitate the set-up of third-party key-storage." (D.I. 17 at 17–18.)

This argument fails because it is premised on Privy's oversimplification of the claims—and refusal to accept as true the FAC's allegations concerning the nature of the claimed invention and its benefit over the prior art. As detailed above, the '321 Patent claims do not merely add a software intermediary to an existing system for third-party key storage; they recite a specific implementation—use of a "non-custodial" authentication system to provide access tokens necessary to request the user's keys from a third-party key storage system, wherein the authentication system does not itself have access to the user's keys—to solve a technological problem arising in computer networks—preventing malicious actors from accessing encryption keys by exploiting vulnerabilities at the user's device or a centralized server. As such, the

'321 Patent claims are analogous to those in *BASCOM*: even if they are found to be directed to an abstract idea, the '321 Patent claims "recite a specific, discrete implementation of the abstract idea" where the "particular arrangement of elements is a technical improvement over prior art" and are "more than a drafting effort designed to monopolize the abstract idea." 827 F.3d at 1350–51 (cleaned up).

That the '321 Patent claims, as a whole, contain an inventive concept, is further supported by cases from this District. For example, in *Network Congestion Solutions, LLC v. United States Cellular Corp.*, the Court denied a motion to dismiss because, although the components of the claimed invention were known, "the claim as a whole (the equipment recited and steps claimed) provides the requisite degree of specificity" and is "directed to a solution for a problem that arises in the computer context." 170 F. Supp. 3d 695, 705 (D. Del. 2016). Similarly, the Court also denied a motion to dismiss because "[a]lthough the patents at issue use computers, the methods recite sufficiently specific steps"—"designed to optimize search results and retrieve target language URLs or documents using search engine queries on the Internet"—so as to ensure that the claims "will not disproportionately tie up the use of the underlying ideas." *Improved Search LLC v. AOL Inc.*, 170 F. Supp. 3d 683, 694 (D. Del. 2016). Like the claims in *Network Congestion* and *Improved Search*, the '321 Patent claims recite a particular arrangement of components, which perform specific steps, to solve a problem that arises in the computer context.

Significantly, "[t]he question of whether a claim element or combination of elements is well-understood, routine and conventional to a skilled artisan in the relevant field is a question of fact" that must be proven by clear and convincing evidence. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1368 (Fed. Cir. 2018). Privy's step two arguments rest on two different factual premises,

each of which controverts the well-pleaded allegations of the FAC. Because, at this juncture, the Court must accept the FAC's factual allegations as true and draw all reasonable inferences in Magic's favor, each of Privy's controverted presumptions requires denial of its motion.

First, Privy presumes that the prior art third-party HSM system was routine and conventional, apparently because it was in the prior art. It is well-established, however that "the mere fact that something is disclosed in a piece of prior art, for example, does not mean it was well-understood, routine, and conventional." *Berkheimer*, 881 F.3d at 1369. The allegations of the FAC demonstrate that the third-party key storage system was not in fact routine and conventional in the pertinent field, including because it was not reasonably available to the users who benefit from the technological solution supplied by Magic's invention (*see supra* at 5). Privy identifies nothing in the record that suggests otherwise—and, even if it had, that would at best create a factual dispute that precludes dismissal. *See id*. (holding that "whether something is well-understood, routine, and conventional to a skilled artisan at the time of the patent is a factual determination" and reversing summary judgment in view of such a factual dispute).

Second, Privy's position is also premised on its own view of the world concerning how the claimed invention supposedly failed to improve upon the prior art—factual premises that, again, ignore and controvert Magic's assertions in the FAC. *Compare* D.I. 17 at 13–14 (Privy asserts that Magic admits that "having a user generate keys locally and then store then with a third-party key storage system was well known" and thus admits that "it was known in the prior art for authentication systems not to have access to the user's keys"), *with* FAC ¶¶ 27, 30 (the prior art third-party key storage system required the user to interface directly with the third party and did not involve any authentication system that could have had access to the user's keys). Each of these factual disputes independently precludes dismissal on the pleadings. *See Aatrix*,

882 F.3d at 1127–28 (claims should not have been dismissed without leave to amend because allegations in the complaint "that the claimed combination improves the functioning and operation of the computer itself" "contradict[ed] the district court's conclusion that the claimed combination was conventional or routine"); *Pure Data Sys., LLC v. Ubisoft, Inc.*, 329 F. Supp. 3d 1054, 1066–67 (N.D. Cal. 2018) (whether particular method of updating a data store as reflected in the "*ordered combination of elements*" recited in the claims "are non-generic and non-conventional in the industry" was a question of fact).

C. At Minimum, Magic Should Be Granted Leave to Amend

Even if the Court grants the motion to dismiss, Magic should be allowed leave to amend because Privy has failed to show that amendment would be futile. *Shane v. Fauver*, 213 F.3d 113, 115 (3d Cir. 2000) ("[L]eave to amend generally must be granted unless the amendment would not cure the deficiency."); *see also* Fed. R. Civ. P. 15(a) (leave to amend should be "freely give[n]"). Indeed, Privy does not address futility at all. Moreover, as detailed above, Privy's arguments appear to be premised on a misunderstanding of the claimed invention and prior art described in the operative complaint. To the extent the Court adopts Privy's view, Magic should be allowed leave to amend the complaint to plead additional facts that correct those misunderstandings, as explained in this brief. *See Arendi S.A.R.L. v. HTC Corp.*, No. CV 12-1600-LPS, 2020 WL 7360155, at *10 (D. Del. Dec. 15, 2020) (leave should be granted where the court cannot say that that amendment would be futile, even if the court is skeptical about the patentee's ability to plead its claims).

VI. CONCLUSION

For the foregoing reasons, the Court should deny Privy's motion to dismiss and find the '321 Patent not invalid under 35 U.S.C. § 101. At minimum, the Court should grant Magic leave to amend because Privy has not demonstrated that amendment would be futile.

DATED: February 5, 2024

MCCARTER & ENGLISH, LLP

/s/ Alexandra M. Joyce

Daniel M. Silver (#4758)
Alexandra M. Joyce (#6423)
Renaissance Centre
405 N. King Street, 8th Floor
Wilmington, DE 19801
T: (302) 984-6300
dsilver@mccarter.com
ajoyce@mccarter.com

Attorneys for Plaintiff
Magic Labs, Inc.

OF COUNSEL:

Daralyn J. Durie
Ragesh K. Tangri
Timothy C. Saulsbury
Michael Burshteyn
Joyce C. Li
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, CA 94105
(415) 268-7000

Sara Doudar
MORRISON & FOERSTER LLP
707 Wilshire Blvd., Suite 6000
Los Angeles, CA 90017
(213) 892-5200